UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,075	10/16/2003	Bhawani Sapkota	72255/00004	8930

23380 7590 05/14/2007

TUCKER, ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1414

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
05/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/687,075	SAPKOTA ET AL.	
	Examiner	Art Unit	
	Canh Le	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☒ Claim(s) *22-26* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10/16/2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/27/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the application filed on 10/16/2003. Claims 1-26 are pending and have been examined.

Claim Objections

The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claim 22 recites "An article of manufacture embodies in a computer-readable medium..." been renumbered 23.

Misnumbered claim 23 been renumbered 24.

Misnumbered claim 24 been renumbered 25.

Misnumbered claim 25 been renumbered 26.

Misnumbered claim 26 been renumbered 27.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 17 and 19-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 17 recites the limitation "embedding the information element into a header". A meaning of "header" could not be found in the specification. Its meaning is unclear. This ambiguity renders claim 17 indefinite.

Claim 19 recites the limitation "authenticating the header". A meaning of "authenticating header" could not be found in the specification. Its meaning is unclear. This ambiguity renders claim 19 indefinite.

Claim 21 recites the limitation "a handshake protocol". A meaning of "a handshake protocol" could not be found in the specification. Its meaning is unclear. This ambiguity renders claim 21 indefinite.

Claims 20-22 are also rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 23-27 are rejected under 35 U.S.C. 101 because the claims are directed to non-statutory subject matter.

Claim 23 recites "An article of manufacture embodies in a computer-readable medium...". The computer-readable medium includes carrier wave/pulse (see paragraph [0014] of the specification) and " a carrier wave/pulse" is, per se, non-statutory.

Claims 24-27 are also rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Cisco Systems, " A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite", 2002, hereinafter Cisco.

As per claim 1, 13:

Cisco teaches a method/ a system for securing management frames, the method comprising the steps of:

(a) establishing an authenticated relationship between a transmitter and a

receiver on a network **[pg. 2, section 2.2. 802.11 Station Authentication; fig. 1; authentication in the specification 802.11 is based on authenticating a wireless station or device instead of authenticating a user. Figure 1 shows authentication process between a wireless station and an access point].**

(b) generating a key **[pg. 21, section 4.1.3.3. Broadcast Key Rotation; broadcast keys are send from an access point to the a client];**

(c) deriving an information element based upon the key for signing a management frame packet transmitted on the network **[pg. 12, section 3.2 Statistical Key Derivation - Passive Network Attacks; a WEP key could be derived by passively collecting particular frames from a wireless LAN"; pg. 18, fig. 24; access point send client broadcast key information which transmits on a network];**

(d) embedding the information element into the management frame packet **[pg. 19, fig. 25, section 4.1.3.1. Message Integrity Check (MIC); fig. 26; MIC adds two new fields to a wireless frame: a sequence number and an integrity check field];**

(e) transmitting the management frame packet to the receiver **[pg. 3; fig. 2; a probe request frame (i.e. management frame) is sent on every channel a client supports in an attempt to find all access points in range that match SSID and client-requested data rates].**

(f) receiving the management frame packet **[pg. 3; "all access point that are in range and match the probe request criteria will respond with a probe**

response frame containing synchronization information and point load"];

and

(g) validating the information element in the received management frame packet **[pg. 3; "all access point that are in range and match the probe request criteria will respond with a probe response frame containing synchronization information and point load"; matching the probe request criteria is equivalent to validating the information element].**

As per claim 2, 14:

Cisco teaches the method/ the system set forth in claim 1 wherein the information element includes a message integrity check information element **[pg. 19, fig. 25, section 4.1.3.1. Message Integrity Check (MIC); pg. 20, fig. 26; MIC adds two new fields to a wireless frame: a sequence number and an integrity check field];**

As per claim 3:

Cisco teaches the method set forth in claim 1 further comprising the steps of:

(a) generating a replay protection value for signing the management frame packet **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. Generating a replay protection value for signing the**

management frame is equivalent to increasing in value on the per-frame]; and

(b) adding the replay protection value into the management frame packet prior to transmitting **[pg. 20, fig. 26; a sequence number (SEQ) is added in WEP Frame format].**

As per claim 4:

Cisco teaches the method set forth in claim 3 further comprising the step of validating the replay protection value **[pg. 19, section 4.1.3. Data Privacy with TKIP and section 4.1.3.1. Message Integrity Check; "MIC adds a sequence number field to the wireless LAN. The access will drop frames received out of order"; "the MIC field provides a frame integrity check not vulnerable to the same mathematical shortcomings as an IVC"].**

As per claim 5:

Cisco teaches the method set forth in claim 1 wherein the step of generating a key is concurrent with the step of establishing an authenticated relationship **[pg. 18, figure 24; a derived key is concurrent in Client Authentication RADIUS server between client and RADIUS server].**

As per claim 6:

Cisco teaches the method set forth in claim 1 wherein the step of establishing an authenticated relationship further includes employing a key establishment

protocol **[pg. 18, figure 24; a derived key is concurrent in Client Authentication RADIUS server between client and RADIUS server; pg. 33, item 4.; "The access point forward the EAP Identity Response to the AAA server using a RADIUS protocol message with Cisco vendor-specific attributes"].**

As per claim 7:

Cisco teaches the method set forth in claim 1 wherein the step of validating the information element further comprises the step of comparing the information element with a locally derived information element established by the receiver **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. An information element is included a sequence number; access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number].**

As per claim 8:

Cisco teaches the method set forth in claim 2 wherein the step of validating the information element further comprises the step of comparing the message integrity check information element of the received management frame packet with a locally derived message integrity check information element established by the receiver **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires**

the use of Cisco clients and access points"; Modifications to any of the fields will result in a discrepancy in the calculated Message Integrity Check (MIC) on the receiver. As a result the receiver will drop the frame"].

As per claim 9:

Cisco teaches the method set forth in claim 3 wherein the step of validating the information element further comprises the step of comparing the replay protection value of the received management frame packet with a locally derived replay protection value established by the receiver **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. Access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number. A sequence number is equivalent a replay protection value].**

As per claim 10:

Cisco teaches the method set forth in claim 1 wherein the receiver includes an access point **[pg. 2, fig. 1; a client and access point authentication process].**

As per claim 11:

Cisco teaches the method set forth in claim 1 wherein the transmitter includes a wireless client **[pg. 2, fig. 1; a client and access point authentication process].**

As per claim 12:

Cisco teaches the method set forth in claim 2 further comprising the step of generating the message integrity check value for the management frame packet prior to transmitting **[pg. 19, fig. 25, section 4.1.3.1. Message Integrity Check (MIC); pg. 20, fig. 26; MIC adds two new fields to a wireless frame: a sequence number and an integrity check field; It is inherent that MIC generates ICV before adding into a wireless frame prior to transmitting].**

As per claim 15:

Cisco further teaches the system set forth in claim 14 wherein the information element further includes a replay protection value **[pg. 20, figure 26; a sequence number (SEQ) is included in WEP frame format].**

As per claim 16:

Cisco teaches the system set forth in claim 13 wherein the means for transmitting the management frame packet is an IEEE 802.11 protocol **[pg. 20, figure 26; 802.11 header is included in a WEP frame format].**

As per claim 17:

Cisco teaches the system set forth in claim 13 wherein the means for adding includes means for embedding the information element into a header of the management frame packet **[pg. 20, figure 26; MIC and SEQ are added a WEP frame format].**

As per claim 18:

Cisco teaches the method set forth in claim 14, wherein the message integrity check information element uniquely identifies the management frame communication to the authenticator **[pg. 20, "The Cisco implementation of per-packet ... and processed normally (Figure 28); page 21, Per-packet keying ... packet keys will be generated"; per-packet keying will not generated the same packet key as unique IV/based WEP key pairs are used].**

As per claim 19:

Cisco teaches a method for preventing IEEE 802.11 session disruption on a network, comprising the steps of:

(a) establishing a communication link between an access point and a wireless client on the network **[pg. 2, section 2.2 802.11 Station Authentication; client and access point authentication process].**

(b) creating a trust relationship between the access point and the wireless client such that the wireless client adapted to securely access the network **[pg. 2, section 2.2 802.11 Station Authentication; client and access point authentication process]**;

(c) establishing a client-specific key for signing a management frame packet configured to be transmitted between the access point and the wireless client **[pg. 16, section 4. Secure 802.11 Wireless LANs with Cisco Wireless Security Suite; "per-packet keying provides every frame with a new and unique WEP key that mitigates WEP key derivation attacks"]**

(d) generating a message integrity check value based upon the client-specific key **[pg. 19, section 4.1.3. Data Privacy with TKIP; TKIP provides two majors enhancements to WEP: MIC and per-packet keying for all WEP-encrypted data frames];**

(e) calculating a replay protection value for signing the management frame packet **[pg. 20, "a sequence number is a sequential counter that increases in value on a per-frame, per-association basis"].**

(f) embedding the message integrity check value and the replay protection value into a header of the management frame packet **[pg. 19, section 4.1.3.1 Message Integrity Check; a MIC adds two new field to a wireless frame: a sequence number and an integrity check field before transmitting]**;

(g) transmitting the header to the access point **[pg. 19, section 4.1.3.1 Message Integrity Check; a MIC adds two new field to a wireless frame: a sequence number and an integrity check field before transmitting]** and

(H) authenticating the header **[pg. 16, section 4; a MIC function provides effective frame authenticity to mitigates man-in-the-middle vulnerabilities"].**

As per claim 20:

Cisco teaches the method set forth in claim 19 further including the step, concurrent with the step of transmitting the header, transmitting the management frame packet **[pg. 20, fig. 26; MIC, SEQ, and 802.11 header are included in a WEP frame format].**

As per claim 21:

Cisco teaches the method set forth in claim 19 wherein a handshake protocol is utilized between the access point and the wireless client in the step of creating a trust relationship **[pg. 2, fig. 1; section 2.2. 802.11 Station Authentication; client and access point authentication process using a request/response protocol].**

As per claim 22:

Cisco teaches the method set forth in claim 19 wherein the step of authenticating further comprises the steps of:

(a) calculating a local replay protection value **[pg. 20, fig. 26; "a sequence number is a sequential counter that increases in value on a per-frame, per-association basis"].**

(b) generating a local message integrity check value **[pg. 20, fig. 27 MIC value derivation. "Modification to any of the fields will result in discrepancy in the calculated MIC on the receiver"];**

(c) comparing the received replay protection value with the local replay protection value **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the**

use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. Access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number. A sequence number is equivalent a replay protection value]; and

(d) comparing the received message integrity check value with the local message integrity check value **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; Modifications to any of the fields will result in a discrepancy in the calculated Message Integrity Check (MIC) on the receiver. As a result the receiver will drop the frame"].**

As per claim 23:

Cisco teaches an article of manufacture embodied in a computer-readable medium for use in a processing system for authenticating management frame packets communicated to and/or from a network, the article comprising:

(a) an authentication logic for causing the processing system to create a trusted relationship between a transmitter and a receiver **[pg. 2, section 2.2. 802.11 Station Authentication; fig. 1; authentication in the specification 802.11 is based on authenticating a wireless station or device instead of authenticating a user. Figure 1 shows authentication process between a wireless station and an access point]**;

(b) a key generation logic for causing the processing system to generate a secure key for encrypting and signing an electronic management frame packet

transmitted on the network **[pg. 21, section 4.1.3.3. Broadcast Key Rotation; broadcast keys are send from an access point to the a client; pg. 12, section 3.2 Statistical Key Derivation - Passive Network Attacks; a WEP key could be derived by passively collecting particular frames from a wireless LAN"; pg. 18, fig. 24; access point send client broadcast key information which transmits on a network]**;

(c) a message integrity check generation logic for causing the processing system to generate a message integrity check for signing the electronic management frame packet transmitted on the network **[pg. 19, fig. 25, section 4.1.3.1. Message Integrity Check (MIC); pg. 20, fig. 26; MIC adds two new fields to a wireless frame: a sequence number and an integrity check field]**;

(d) a replay protection value generation logic for causing the processing system to generate a replay protection value for signing the electronic management frame packet transmitted on the network **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. Generating a replay protection value for signing the management frame is equivalent to increasing in value on the per-frame]**;

(e) a signing logic for causing the processing system to embed the message integrity check and the replay protection value into a header of the management frame packet **[pg. 19, section 4.1.3.1 Message Integrity Check; a MIC adds**

two new field to a wireless frame: a sequence number and an integrity check field before transmitting];

(f) a data transmitting logic for causing the processing system to transmit the header and the electronic management frame packet via the network **[pg. 3; fig. 2; a probe request frame (i.e. management frame) is sent on every channel a client supports in an attempt to find all access points in range that match SSID and client-requested data rates]**; and

(g) a message receiving logic for causing the processing system to verify the received message integrity check and the replay protection value included in the header **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; Modifications to any of the fields will result in a discrepancy in the calculated Message Integrity Check (MIC) on the receiver. As a result the receiver will drop the frame"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. An access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number].**

As per claim 24:

Cisco further teaches the article as set forth in claim 23 wherein the data transmitting logic includes an IEEE 802.11 protocol **[pg. 20, figure 26; 802.11 header is included in a WEP frame format].**

As per claim 25:

Cisco further teaches the article as set forth in claim 23 wherein the replay protection value generation logic includes a sequential counter **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. Access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number. A sequence number is equivalent a replay protection value].**

As per claim 26:

Cisco further teaches the article as set forth in claim 23 wherein the message receiving logic further includes logic for causing a processing system to compare a received message integrity check with a locally generated message integrity check **[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; Modifications to any of the fields will result in a discrepancy in the calculated Message Integrity Check (MIC) on the receiver. As a result the receiver will drop the frame"]**.

As per claim 27:

Cisco further teaches the article as set forth in claim 23 wherein the message received logic further includes logic for causing a processing system to compare a received reply protection value with a locally calculated replay protection value

[pg. 20, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. Access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number. A sequence number is equivalent a replay protection value].

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

U.S. Patent Application Publication No. 20040030895 A1 to Tachikawa, Hirohide;

U.S. Patent Application Publication No. 20020191572 A1 to Weinstein, Stephen B. et al.;

U.S. Patent Application Publication No. 20030112977 A1 to Ray, Dipankar et al.;

U.S. Patent No. US 5524052 A to Augustine; Kurt E. et al.

Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker, "Security Flaws in 802.11 Data Link Protocols", COMMUNICATION OF THE ACM, vol. 46, no. 5, May 2003 pages 35-39.

Dennis Eaton, Intersil, "Diving into the 802.11i Spec: A Tutorial", November 26, 2002, pages 1-7.

Niels Ferugson and MacFergus, "Michael: an improved MIC for 802.11 WEP", Jan 17, 2002, pages 1-18.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le

May 2, 2007

TAGHI ARANI
PRIMARY EXAMINER
5/10/07